Weight Enumerators of Codes over $\mathbf{Z}/2k\mathbf{Z}$ (Algebraic Combinatorics)

AUTHOR(S):

Oura, Manabu

CITATION:

Oura, Manabu. Weight Enumerators of Codes over $\mathbf{Z}/2k\mathbf{Z}$ (Algebraic Combinatorics). 数理解析研究所講究録 1998, 1063: 170-173

ISSUE DATE:

1998-09

URL:

http://hdl.handle.net/2433/62416

数理解析研究所講究録
1063巻 1998年 170-173

Weight Enumerators of Codes over $\mathbf{Z}/2k\mathbf{Z}$

Manabu Oura （大浦　学）

In this note, we announce some results in [1].

1 Codes over $\mathbf{Z}/2k\mathbf{Z}$ and lattices

We set $R := \mathbf{Z}/2k\mathbf{Z}$. A linear codes $\mathcal{C}$ of length n over R is an additive subgroup of R^n. The Euclidean weight $wt_E(x)$ of a vector $x = (x_1, \cdots, x_n)$ is $\sum_{i=1}^{n} x_i^2 \mod 4k$. We define the inner product of x and y in R^n by $< x, y >= x_1y_1 + \cdots + x_ny_n(\mod 2k)$, where $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$. The dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp} = \left\{ x \in R^n | < x, y >= 0, {}^{\forall} y \in \mathcal{C} \right\}.$$

$\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$. We define a Type II code over R as a self-dual code with Eudidean weights divisible by $4k$. We consider the natural projection ρ from $\mathbf{Z}$ to R, then this map induces the map (also we denote ρ) from $\mathbf{Z}^n$ to R^n. We set $\Lambda(\mathcal{C}) = \frac{1}{\sqrt{2k}}\rho^{-1}(\mathcal{C})$.

Theorem 1 *If $\mathcal{C}$ is self-dual code of length n over R, then the lattice $\Lambda(\mathcal{C})$ is an n-dimensioal unimodular lattice. Moreover if $\mathcal{C}$ is Type II, then the lattice $\Lambda(\mathcal{C})$ is an even unimodular lattice.*

Proposition 2 *There exists a Type II code of length n over R if and only if n is a multiple of eight.*

Remark 3 For $k = 2$, Type II codes of lengths 8 and 16 are classified.

2 Weight enumerators and modular forms

Definition 4 For a code $\mathcal{C}$ over R, we define the g-th complete weight enumerator of $\mathcal{C}$ by

$$\mathfrak{C}_{\mathcal{C}}^{g}(x_a \text{ with } a \in R^g) := \sum_{C_1, \cdots, C_g \in \mathcal{C}} \prod_{a \in R^g} x_a^{n_a(c_1, \cdots, c_g)}$$

where $n_a(c_1, \cdots, c_g)$ denotes the number of i satisfying $a = (c_{1i}, \cdots, c_{gi})$.

We define a relation $\sim$ in R^g by

$$a \sim b \Leftrightarrow a = b \text{ or } a = -b,$$

where $a, b \in R^g$. We set $\overline{R^g} := R^g / \sim$.

Definition 5 For a code $\mathcal{C}$ over R, we define the g-th symmetrized weight enumerator of $\mathcal{C}$ by

$$\mathfrak{S}_{\mathcal{C}}^{g}(y_{\overline{a}} \text{ with } \overline{a} \in \overline{R^g}) := \sum_{c_1,\cdots,c_g \in \mathcal{C}} \prod_{\overline{a} \in \overline{R^g}} y_{\overline{a}}^{n_{\overline{a}}(c_1,\cdots,c_g)},$$

where $n_{\overline{a}}(c_1,\cdots,c_g)$ denotes the number of i satisfying $\overline{a} = \overline{(c_{1i},\cdots,c_{gi})}$.

We consider the following procedure ϕ: for $g = (g_{ab})_{a,b \in R^g}$, we set

$$\phi(g) := \left(\sum_{d \in R_{2k}^g \text{ with } \overline{d}=\overline{b}} g_{ad} \right)_{\overline{a},\overline{b} \in \overline{R^g}}$$

Theorem 6 *For a code $\mathcal{C}$ over R, we have*

$$\mathfrak{C}_{\mathcal{C}^\perp}^{g}(x_a) = \frac{1}{|\mathcal{C}|^g} T \cdot \mathfrak{C}_{\mathcal{C}}^{g}(x_a),$$

and

$$\mathfrak{S}_{\mathcal{C}^\perp}^{g}(x_a) = \frac{1}{|\mathcal{C}|^g} \phi(T) \cdot \mathfrak{S}_{\mathcal{C}}^{g}(x_a),$$

where $T = (\eta_{2k}^{<a,b>})_{a,b \in R^g}$.

For a symmetric integral matrix S of size $g \times g$, we define $D_S := \operatorname{diag}\left(\eta_{4k}^{S[a]} \text{ with } a \in R^g\right)$. Let us define

$$G_{g,k}^{8} := \left\langle \left(\frac{\eta_8}{\sqrt{2k}}\right)^g T, D_S, \eta_8 \right\rangle,$$

$$H_{g,k}^{8} := \left\langle \left(\frac{\eta_8}{\sqrt{2k}}\right)^g \phi(T), \phi(D_S), \eta_8 \right\rangle,$$

where S runs over all symmetric integral matrices of size $g \times g$ and η_8 denotes the primitive 8-th root of unity.

Theorem 7 *For any Type II code C over R, the g-th complete (resp. symmetrized) weight enumerator is invariant under the action of the group $G_{g,k}^8$ (resp. $H_{g,k}^8$).*

We define the thetas $f_a^{(k)}(\tau)$ by

$$f_a^{(k)}(\tau) := \sum_{x \in R^g} e^{2\pi i k \tau[x+\frac{1}{2k}a]}, a \in R^g, \tau \in \mathcal{H}_g$$

where $\mathcal{H}_g$ denotes the Siegel upper harf space of degree g.

The theta for a lattice L in genus g is denoted by

$$\theta_L^g(\tau) := \sum_{x_1,\cdots,x_g \in L} \Pi_{1 \le i,j \le g} e^{\pi i <x_i,x_j> \tau_{ij}}, \quad \tau = (\tau_{ij}) \in \mathcal{H}_g$$

Because of the identity $f_a^{(k)}(\tau) = f_{-a}^{(k)}(\tau)$, we may define $f_{\overline{a}}^{(k)}(\tau) := f_a^{(k)}(\tau)$. Direct computation shows

$$\mathfrak{C}_{\mathcal{C}}^{g}(f_a^{(k)}(\tau)) = \mathfrak{S}_{\mathcal{C}}^{g}(f_{\overline{a}}^{(k)}(\tau)) = \theta_{\Lambda(C)}^{g}(\tau).$$

In particular, we have

Theorem 8 *For any Type II code $\mathcal{C}$, $\mathfrak{C}_{\mathcal{C}}^{g}(f_a(\tau))$ is a Siegel modular form of weight $n/2$ for the Siegel modular group $\Gamma_g = S_{P_{2g}}(\mathbf{Z})$.*

3 Dimension formulas

In this section, we discuss the dimension formulas of the invariant rings of $G_{1,2}^8$ and $H_{1,2}^8$.

First, let us recall the general invariant theory of finite groups. Let G be a finite subgroup of $GL(n;\mathbf{C})$. Then G acts on the polynomial ring $\mathbf{C}[x_1,\ldots,x_n]$ ($\mathbf{C}[x_k]$ for short) naturally, i.e.,

$$A\cdot f(x_1,\ldots,x_n)=f(\sum_{1\le j\le n}A_{1j}x_j,\ldots,\sum_{1\le j\le n}A_{nj}x_j),$$

where $f\in\mathbf{C}[x_k]$ and $A=(A_{ij})_{1\le i,j\le n}$. There exists a *homogenueous system of parameters* $\{\theta_1,\ldots,\theta_n\}$ such that the invariant ring $\mathbf{C}[x_k]^G$ is finitely generated free $\mathbf{C}[\theta_1,\ldots,\theta_n]$-module. The invariant ring has the *Hironaka decomposition*

$$\mathbf{C}[x_k]^G=\oplus_{1\le m\le s}g_m\mathbf{C}[\theta_1,\ldots,\theta_n],\ g_1=1$$

The invariant ring is an graded ring and the dimension formula is defined by

$$\Phi_G(t)=\sum_{d\ge 1}\dim\mathbf{C}[x_k]_d^G t^d,$$

where $\mathbf{C}[x_k]_d^G$ is the d-th homogeneous part of $\mathbf{C}[x_k]^G$. The dimension formula for the *Hironaka decomposition* given in the above form is

$$\Phi_G(t)=\frac{1+t^{\deg(g_2)}+\cdots t^{\deg(g_s)}}{(1-t^{\deg(\theta_1)})\cdots(1-t^{\deg(\theta_n)})}.$$

In general, the converse is not true. It is known that we have the identity

$$\Phi_G(t)=\sum_{A\in G}\frac{1}{\det(1-tA)},$$

This was shown by Molien and is sometimes called *Molien series.*

Let $\mathcal{W}_{g,k}$ (res. $\mathcal{S}_{g,k}$) denote the ring generated by the g-th complete (resp. symmetrized) weight enumerators of Type II codes over $\mathbf{Z}/2k\mathbf{Z}$. We denote the d-th homogeneous part of $\mathcal{W}_{g,k}$ (resp. $\mathcal{S}_{g,k}$) by $\mathcal{W}_{g,k}(d)$ (res. $\mathcal{S}_{g,k}(d)$). Theorem 7 says that $\mathcal{W}_{g,k}$ (resp. $\mathcal{S}_{g,k}$) is a subring of $\mathbf{C}[x_k]^{G_{g,k}^8}$ (resp. $\mathbf{C}[x_k]^{H_{g,k}^8}$). We have $\dim\mathcal{W}_{g,k}(d)\le\dim\mathbf{C}[x_k]_d^{G_{g,k}^8}$ and $\dim\mathcal{S}_{g,k}(d)\le\dim\mathbf{C}[x_k]_d^{H_{g,k}^8}$.

$|G_{1,2}^8|=1536$. Magma computation shows that we may have invariant ring has the homogenueous system of parameters with degrees 8, 8, 8, and 24. We have the dimension formula of the invariant ring is:

$$\begin{aligned}\Phi_{G_{1,2}^8}(t)&=1+4t^8+11t^{16}+25t^{24}+48t^{32}+\cdots\\&=(1+t^8+2t^{16}+2t^{24}+t^{32}+t^{40})/(1-t^8)^3(1-t^{24})\\&=(1+t^8)(1+t^{16})^2/(1-t^8)^3(1-t^{24}).\end{aligned}$$

With the help of [6], we have $\dim\mathcal{W}_{1,2}(8)=4$, $\dim\mathcal{W}_{1,2}(16)=11$ and $\dim\mathcal{W}_{1,2}(24)\ge 23$. At the time of writing, the author doesn't know if this invariant ring $\mathcal{W}_{1,2}$ can be generated by the weight enumerators of Type II codes or not.

$|H^8_{1,2}| = 768$. It is proved that the invariant ring $\mathbf{C}[x_k]^{H^8_{1,2}}$ coincides with the ring $\mathcal{S}_{1,2}$ of symmetrized weight enumerators of Type II codes in [2]. The dimension fomula is given by

$$\begin{aligned}\Phi_{H^8_{1,2}}(t) &= 1+2t^8+4t^{16}+7t^{24}+10t^{32}+\cdots \\ &= (1+t^{16})/(1-t^8)^2(1-t^{24}).\end{aligned}$$

References

[1] Bannai, E., Dougherty, S. T., Harada, M., Oura, M., Type II codes, even unimodular lattices and invariant rings, preprint.

[2] Bonnecaze, A., Solé, P., Bachoc, C., Mourrain, B., Type II codes over $\mathbf{Z}_4$.

[3] Bonnecaze, A., Solé, P., Calderbank, A. R., Quaternary quadratic residue codes and unimodular lattices, IEEE Trans. Inform. Theory, 41 no2 (1995), 366–377.

[4] Hammons, Jr., A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Solé, P., The $\mathbf{Z}_4$ linearitu of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory, 40 No.2 (1994), 301–319.

[5] Klemm, M., Selbstduale Codes über dem Ring der ganzen Zahlen modulo 4, Arch. Math., 53 (1989), 201–207.

[6] Pless, P., Leon, J. S., Fields, J., All $\mathbf{Z}_4$ codes of Type II and length 16 are known.

[7] Runge, B., Theta functions and Siegel-Jacobi forms, Acta. Math., 175 (1995), 165–196.

Manabu Oura
Graduate School of Mathematics
Kyushu University
6-10-1, Hakozaki,
Higashi-ku, Fukuoka, 812-8581, Japan
email:ohura@math.kyushu-u.ac.jp